NOT FOR PUBLICATION (Docket Nos. 79, 81, 82)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY
CAMDEN VICINAGE

RUSS SMITH, pro se,	:	
Plaintiff,	:	Civil No. 09-4567 (RBK/KMW)
v.	:	**OPINION**
TRUSTED UNIVERSAL STANDARDS IN ELECTRONIC TRANSACTIONS, INC. (d/b/a TRUSTe, Inc.), MICROSOFT, INC., CISCO SYSTEMS, INC., and COMCAST CABLE COMMUNICATIONS, LLC,	:	
Defendants.	:	

KUGLER, United States District Judge:

This matter arises out of the allegedly improper monitoring and blocking of email communications. Presently before the Court is the motion to dismiss filed by Defendants Microsoft, Inc. ("Microsoft"), Cisco Systems, Inc. ("Cisco"), and Comcast Cable Communications, LLC ("Comcast") for failure to state a cause of action under Federal Rule of Civil Procedure 12(b)(6). On January 18, 2011, the Court converted the motion to dismiss into a motion for summary judgment pursuant to Federal Rule of Civil Procedure 12(d). For the reasons discussed below, the motion for summary judgment is **GRANTED**.

I. BACKGROUND

Plaintiff is a subscriber of Comcast's internet services and operates an email server external to the Comcast network. Cisco is a publicly traded company that develops internet

protocol-based networking solutions for individuals, companies, and countries.[1] Cisco owns Cisco IronPort Systems, LLC ("IronPort"), an email and web security company. IronPort operates the SenderBase service. Through the use of an elaborate data collection system, SenderBase gathers information about individual internet protocol ("IP") addresses. After gathering and analyzing data for each IP address, SenderBase assigns a "reputation score" to the IP address. A reputation score predicts the likelihood that email from a given IP address is spam. SenderBase uses over 120 factors to determine each reputation score including, but not limited to, the number of end-user complaints associated with an IP address and the frequency of URLs appearing in spam or viral messages.

Microsoft is a publicly traded computer software and services company. Microsoft operates a service known as FrontBridge as part of its Exchange Hosted Services ("EHS").[2] Microsoft's EHS provides spam and virus filtering software. Microsoft's EHS datasheet provides a detailed description of its spam and virus filtering software. The datasheet contains a diagram that depicts an elaborate system that intercepts, filters, and then delivers emails to intended recipients. Subscribers set their email preferences to provide EHS with guidance regarding how it should filter their e-mail. In order to manage those preferences, subscribers use their home computers to log into the EHS Administrator Center over the Internet. Subscribers may also direct the Administrative Center to quarantine all of their filtered email. Periodically, subscribers who choose to quarantine their filtered email receive notices from the Spam Quarantine listing all quarantined messages. Subscribers interact with the Spam Quarantine

[1] See http://newsroom.cisco.com/dlls/corpinfo/factsheet.html (last visited March 9, 2011).

[2] Microsoft acquired FrontBridge Technologies Inc. in 2005. Microsoft then changed the name "FrontBridge" to "Exchange Hosted Services," and then "Forefront Online Security for Exchange." Thereafter, Microsoft changed the name "Forefront Online Security for Exchange" to its current name, "Forefront Online Protection for Exchange." See Cert. of Terence M. Zink ¶ 2.

computer server by reviewing and releasing quarantine messages. Plaintiff claims that FrontBridge also compiles information about internet email services by collecting email messages and creating IP address "blacklists." (Compl. ¶ 85). Plaintiff also claims that Microsoft "blocks e-mail communications originating from the IP addresses on the blacklists from reaching . . . [its] client[s]." (Id. ¶ 38).

Plaintiff alleges that he experienced difficulty sending outgoing email on two separate occasions in 2008 and 2009. In July 2008, Plaintiff alleges that his outgoing emails were blocked because he was placed on a "blacklist" operated by FrontBridge. A few weeks later, Plaintiff claims that Comcast blocked his outgoing email a second time. After the first blockage, Plaintiff alleges that he contacted Microsoft to determine why he was unable to send email. Microsoft provided Plaintiff with no explanation, but instead promised to provide him with the information it collected from his email. However, Microsoft failed to supply Plaintiff with that information. When Plaintiff contacted Microsoft after the second blockage, Microsoft failed to respond.

In March 2009, Plaintiff discovered that he was unable to send email through his email server. As a result, Plaintiff contacted Comcast to determine the reason for the blockage. Comcast informed Plaintiff that it detected outgoing "spam" sent from his account. Subsequently, Comcast stated that it blocked Plaintiff's outgoing email because Plaintiff's IP address received a low reputation score from Cisco's IronPort service. Thereafter, Plaintiff asked both Comcast and Cisco for the reason why Cisco gave Plaintiff's account a poor reputation score. Plaintiff alleges that both parties refused to provide that information. Plaintiff also alleges that both Comcast and Cisco denied Plaintiff access to all of his account information with the exception of his customer invoices. Plaintiff also claims that Comcast blocked his email

a few weeks later, but failed to provide him with an explanation for the blockage when asked to do so.

On July 29, 2009, Plaintiff brought a lawsuit against Comcast, Cisco, Microsoft, and TRUSTe[3] in the Superior Court of New Jersey alleging a variety of state law claims and federal statutory claims. Defendants removed the case to the United States District Court for the District of New Jersey on September 4, 2009. (Doc. No. 1). On September 29, 2009, Defendants moved to dismiss all of Plaintiff's claims pursuant to Federal Rule of Civil Procedure 12(b)(6).[4] (Doc. No. 29). On May 4, 2010, this Court dismissed all of Plaintiff's claims without prejudice, (Doc. Nos. 63, 64), and on June 3, 2010, Plaintiff filed the Second Amended Complaint, (Doc. No. 68), alleging the following causes of action:

1) Violation of the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2 et seq. ("NJCFA") (against Comcast, Microsoft, and Cisco);
2) Breach of Contract (against Comcast, Microsoft, and Cisco);
3) Violation of the Federal Wiretap Act, 18 U.S.C. § 2510 et seq. (the "Wiretap Act") (against Microsoft and Cisco);
4) Violation of the New Jersey Wiretapping and Electronic Surveillance Control Act, N.J. Stat. Ann. § 2A:156A-1 et seq. (the "New Jersey Wiretap Act") (against Microsoft and Cisco);
5) Defamation (against Microsoft and Cisco);
6) Violation of the Cable Communications Policy Act, 47 U.S.C. § 551 et seq. (against Comcast); and

[3] Plaintiff dropped all claims against TRUSTe in the Second Amended Complaint.

[4] Plaintiff also filed a Motion to Remand all state law claims on September 18, 2009. The Court denied Plaintiff's Motion to Remand on May 4, 2010. (Doc. No. 64).

7) Violation of Comcast's local franchise agreement with Ocean City, New Jersey.

On July 19, 2010, Defendants moved to dismiss the Second Amended Complaint. (Doc. Nos. 79, 81, 82). On January 18, 2011 the Court converted the motion to dismiss into a motion for summary judgment and gave the parties seven days to submit additional documentation. The parties submitted their papers and the motion is now ripe for review.

II. STANDARD

Defendant originally filed the present motion as a motion to dismiss. When ruling on a motion to dismiss, the Court may only rely on matters within the pleadings. Pryor v. Nat'l Collegiate Athletic Ass'n, 288 F.3d 548, 560 (3d Cir. 2002). If the court relies upon matters outside of the pleadings, it must convert the motion into a motion for summary judgment pursuant to Federal Rule of Civil Procedure 12(d). See Fed. R. Civ. P. 12(d) ("If on a motion under Rule 12(b)(6) or 12(c), matters outside the pleadings are presented to and not excluded by the court, the motion must be treated as one for summary judgment under Rule 56."). Because the parties heavily relied upon documents outside the Second Amended Complaint, the Court issued an order converting Defendants' motion to dismiss into a motion for summary judgment. (Doc. No. 93).

Summary judgment is appropriate where the Court is satisfied that "there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c); see Celotex Corp. v. Catrett, 477 U.S. 317, 330 (1986). A genuine issue of material fact exists only if the evidence is such that a reasonable jury could find for the nonmoving party. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). When the court weighs the evidence presented by the parties, "[t]he evidence of the non-movant is to be believed, and all justifiable inferences are to be drawn in his favor." Id. at 255.

The burden of establishing the nonexistence of a "genuine issue" is on the party moving for summary judgment. Aman v. Cort Furniture Rental Corp., 85 F.3d 1074, 1080 (3d Cir. 1996). The moving party may satisfy its burden either by "produc[ing] evidence showing the absence of a genuine issue of material fact" or by "'showing' – that is, pointing out to the district court – that there is an absence of evidence to support the nonmoving party's case." Celotex, 477 U.S. at 325.

Once the moving party satisfies this initial burden, the nonmoving party must "set out specific facts showing a genuine issue for trial." Fed. R. Civ. P. 56(e). To do so, the nonmoving party must "do more than simply show that there is some metaphysical doubt as to the material facts." Matsushida Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 586 (1986). Rather, to survive summary judgment, the nonmoving party must "make a showing sufficient to establish the existence of [every] element essential to that party's case, and on which that party will bear the burden of proof at trial." Celotex, 477 U.S. at 322. Furthermore, "[w]hen opposing summary judgment, the nonmovant may not rest upon mere allegations, but rather must 'identify those facts of record which would contradict the facts identified by the movant.'" Corliss v. Varner, 247 F. App'x 353, 354 (3d Cir. 2007) (quoting Port Auth. of N.Y. & N.J. v. Affiliated FM Ins. Co., 311 F.3d 226, 233 (3d Cir. 2002)).

In deciding the merits of a motion for summary judgment, the court's role is not to evaluate the evidence and decide the truth of the matter, but to determine whether there is a genuine issue for trial. Anderson, 477 U.S. 249. Credibility determinations are the province of the factfinder, not the district court. BMW, Inc. v. BMW of N. Am., Inc., 974 F.2d 1358, 1363 (3d Cir. 1992).

II. DISCUSSION

A. CDA Immunity

All defendants argue that they are immune to liability under the Communications Decency Act of 1996 ("CDA"), 47 U.S.C. § 230 et seq. The CDA was enacted "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services," 47 U.S.C. § 230(b)(3), and "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material," 47 U.S.C. § 230(b)(4). To further those objectives, the CDA provides "good Samaritan" immunity for systems and programs designed to block and screen offensive material. Under 47 U.S.C. § 230(c)(2), the "provider" or "user" of an "interactive computer service" cannot be held liable for

> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[5]

Under the CDA, courts generally construe the terms "interactive computer service" very broadly. Zango v. Kaspersky Lab, No. 07-0807, 2007 WL 5189857, at *3 (W.D. Wash. Aug. 28, 2007); see Carafano v. Metrosplash.com Inc., 339 F.3d 1119, 1122 (9th Cir. 2003) (noting that "reviewing courts have treated § 230(c) as quite robust, adopting a relatively expansive definition of 'interactive computer service' . . . ."); Batzel v. Smith, 333 F.3d 1018, 1030 n.15

[5] The Court notes that the reference to "paragraph (1)" in 47 U.S.C. § 230(c)(2)(B) appears to be a clerical error. The appropriate reference is to paragraph (A).

(3d Cir. 2003) (citing examples of "interactive computer service(s)" such as on-line auction website, on-line bookstore, newsgroup, on-line stock quotation service, on-line bulletin board, and on-line gossip column). An "interactive computer service" is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2). An "access software provider" is defined as "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." 47 U.S.C. § 230(f)(4).

Section 230(c)(2)(A) provides that the user or provider of an interactive computer service may restrict access to material that the user or provider considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable . . . ." (emphasis added). Importantly, Section 230(c)(2)(A) does not require the user or provider of an interactive computer service to demonstrate that the otherwise "objectionable" material is actually objectionable. Zango, 2007 WL 5189857, at *4. Instead, the provision protects material that the user or provider considers to be objectionable. 47 U.S.C. § 230(c)(2)(A). Users or providers of an interactive computer service may determine that spam is material that is harassing or otherwise objectionable under Section 230(c)(2)(A). Smith v. Trusted Universal Standards in Elec. Transactions, Inc., 09-4567, 2010 WL 1799456, *6 (D.N.J. May 4, 2010) [hereinafter "Smith I"].

Thus, the user or provider of an interactive computer service (or access service provider), who provides information-content providers with the technical means to restrict access to material that the user or provider considers to be (a) obscene, (b) lewd, (c) lascivious, (d) filthy, (e) excessively violent, (f) harassing, or (g) otherwise objectionable, is entitled to immunity under the CDA. Good Samaritan immunity under the CDA applies to all civil claims except claims based on alleged violations of intellectual property law and the Federal Wiretap Act. 47 U.S.C. § 230 (e)(2), (4). Moreover, the CDA also preempts any conflicting state law. 47 U.S.C. § 230(e)(3).

1. Cisco

Cisco argues that it is entitled to CDA immunity. In Smith I, the Court found that although Cisco argued that it was an "access service provider,"[6] it was not entitled to Section 230 immunity because it failed to argue that it was the user or provider of an "interactive computer service" within the meaning of Section 230. 2010 WL 1799456, at *7. Now, Cisco argues that it

[6] Cisco argued that it was an access service provider because it "provide[s] the technical means to restrict access to material." Smith, 2010 WL 1799456, at *7. The Court agrees. 47 U.S.C. § 230(f)(4) provides:

> The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:
> (A) filter, screen, allow, or disallow content;
> (B) pick, choose, analyze, or digest content; or
> (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

The SenderBase fact sheet states that:

> The SenderBase Reputation Score (SBRS) powers IronPort Reputation Filters, the outer layer of defense available to IronPort email security appliance customers to prevent email-based threats from entering their network. Tightly integrated with IronPort's email security appliance, IronPort Reputation Filters allow customers to apply policies – such as blocking known bad senders, throttling suspicious senders and allowing trusted senders to bypass traditional spam filters.

(White Certif. Exh A). Because SenderBase analyzes content and informs customers of legitimate senders and spammers, it certainly falls within the definition of "access service provider" under Section 230(f)(4).

is entitled to immunity under the CDA because it is both the "user" and "provider" of an interactive computer service under Section 230(b)(2)(B). Cisco reasons that it is the "user" of an interactive computer service because SenderBase uses "numerous computer services such as domain name servers and internet service providers." (Def.'s Mot. Br., at 8). Furthermore, Cisco argues that it is the "provider" of an interactive computer service because SenderBase service operates the website www.senderbase.org. The Court agrees.

First, Cisco's website, www.senderbase.org, is an interactive computer service within the meaning of Section 230. As the court noted in Smith I, an access software provider must "provide or enable computer access by multiple users to a computer server." Smith I, 2010 WL 1799456, at *7 (quoting 47 U.S.C. § 230(f)(2)). Generally, websites are considered interactive computer services because they allow numerous users to access and use their services such as searchable databases. See Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1162 n.6 (9th Cir. 2008) (finding that defendant's website was an "interactive computer service" because although it did not provide or enable access to the Internet, "[t]hrough the Internet, many thousands of members are able to access and use a searchable database maintained on [the defendant's] computer services."); see also Zango, 2007 WL 5189857, at *3 ("All internet-based interactions necessarily involve computers interacting with one another to facilitate communication."). Thus, because www.senderbase.org is a website, it is an interactive computer service within the meaning of Section 230.

Second, the Court finds that Cisco is both the "user" and "provider" of an interactive computer service. It is clear that Cisco is the "user" of an interactive computer service because it uses the website www.senderbase.org to publish IP address reputation scores. See Optinrealbig.com, LLC v. Ironport Sys., Inc., 323 F. Supp. 2d 1037, 1047 (N.D. Cal. 2004)

(finding that antispam website was the user of an interactive computer service because it collected reports and posted them on a website). Cisco is also the "provider" of an interactive computer service because it operates the website www.senderbase.org. See Zango Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1175 (9th Cir. 2009) (finding that defendant antivirus software was a provider of an interactive computer service because it "provid[es] . . . customers with online access to its update servers."); Optinrealbig.com, 323 F. Supp. 2d at 1047 (finding that anti-spam website, that collected and reported complaints of excessive spam to internet service providers was entitled to Section 230 immunity).

Third, the Court finds that Cisco's SenderBase service "make[s] available to information content providers . . . the technical means to restrict access to" harassing and objectionable material. 47 U.S.C. § 230(c)(2)(B). As previously mentioned, the user or provider of an interactive computer service need not demonstrate that "objectionable material" is actually objectionable in order to be immune from liability under the CDA. Zango, 2007 WL 5189857, at *4. Instead, the provision defines "objectionable" material as material that the provider or user considers to be objectionable. 47 U.S.C. § 230(c)(2)(A). The user or provider of an interactive computer service may determine that spam email is harassing or objectionable material within the meaning of Section 230. Smith I, 2010 WL 1799456, at *6. Because SenderBase helps information content providers restrict access to spam email, SenderBase is a service that provides information content providers with the means to restrict access to harassing or objectionable material within the meaning of Section 230(c)(2)(A).

In sum, because Cisco is both the user and operator of an interactive computer service that provides Comcast with the technical means to restrict access to unwanted spam, Cisco is

entitled to immunity under the CDA as a matter of law. Accordingly, the Court will grant Cisco summary judgment on Plaintiff's defamation, NJCFA, and breach-of-contract claims.[7]

2. Microsoft

In Smith I, the Court found that although Microsoft argued that it was an "access service provider," it was not entitled to Section 230 immunity because it failed to argue that by operating the EHS service, it was the user or provider of an access software provider that "provide[s] or enable[s] computer access by multiple users to a computer server." Smith I, 2010 WL 1799456, at *7 (quoting 47 U.S.C. § 230(f)(2)). Microsoft now argues that it is the user or provider of an "interactive computer service" because its EHS service filters emails sent to customers through a Microsoft interactive server. Moreover, Microsoft claims that it is an access software provider because it provides enabling tools that filter and disallow content in the form of spam email messages and viruses. The Court agrees.

The evidence demonstrates that Microsoft is the user or provider of an interactive computer service that provides or enables computer access by multiple users to a computer server. As previously mentioned, the statutory definition of an interactive computer service includes an "access software provider." An access service provider is defined as "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." 47 U.S.C. § 230(f)(4) (emphasis added). Microsoft's EHS technology falls precisely within the CDA's definition of an access software provider. The EHS Privacy Statement

[7] The Court notes that Plaintiff's breach of contract and defamation claims are dismissed because they specifically relate to Cisco's SenderBase service. Plaintiff defamation claim is based upon the fact that Cisco publishes IP scores. (Second Am. Compl. ¶ 23). Plaintiff's breach of contract claim is based on the fact that Cisco refused to provide Plaintiff with the information that it used to calculate the reputation score for the IP address assigned to Plaintiff by Comcast. (Id. ¶ 3).

provides the following description of Microsoft's email filtering service: "Exchange Hosted Filtering analyzes e-mail for spam, viruses and other malware, as well as policy violations as defined by the administrator, before delivering the e-mail." (Second Am. Compl. Ex. X, at 1). The exhibit attached to the Certification of Mr. Terence M. Zink, a Microsoft employee and the Program Manager of Antispam, further illustrates how Microsoft's EHS filters and blocks objectionable material. (Cert. of Terence M. Zink Ex. A). Mr. Terence M. Zink describes the EHS service as follows:

> E-mail sent over the Internet to a subscriber first goes to one of these computer servers, which we call Mail Hosts, to be filtered for spam and other objectionable material according to the subscriber's preferences. E-mail that passes through the filter is delivered to the subscriber's mailbox. E-mail that fails to pass through the filter is either rejected, marked as spam and quarantined on other computer servers known as Spam Quarantine servers, or marked and sent to the subscribing organization for review.

(Id. ¶ 4). Thus, because Microsoft's EHS service is software that "filter[s], screen[s], and disallow[s]" content it is an access software provider under the CDA.

Microsoft's EHS also "provide[s] or enable[s] computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2)). Mr. Zink provided the following description of how EHS enables multiple users to access its computer servers:

> [T]he service now known as Forefront Online Protection for Exchange has been an interactive computer service that enables multiple users to access computer servers. The [EHS] service utilizes more than a thousand computer servers around the world. Those servers are connected to the Internet and stand between subscribers and e-mail sent over the Internet to those subscribers. E-mail sent over the Internet first goes to one of these computer servers, which we call Mail Hosts, to be filtered for spam or other objectionable material according to the subscriber's preferences.

(Cert. of Terence M. Zink ¶ 4). Thus, multiple users access EHS servers whenever they send

outgoing email, or whenever they receive incoming email. Moreover, subscribers interact with computer servers when they manage their email preferences:

> To manage their e-mail preferences, subscribers use their own computers connected to the Internet to access a computer server known as an Administrator Center and log in. Once logged in, they interact with the Administrative Center computer server by establishing and updating their preferences for how their e-mail should be filtered. Multiple subscribers log in over the Internet and access each Administrator Center computer server interactively.
> . . .
> Subscribers who set their preference in the Administrative Center computer server to quarantine filtered e-mail receive periodic notices from a Spam Quarantine computer server listing the quarantined messages. Subscribers can review and release the quarantined messages by clicking on links in the notices. In so doing, they interact with the Spam Quarantine computer servers. Multiple subscribers interact with each Spam Quarantine computer server in this way.

(Id. ¶ 5). Thus, subscribers also access EHS computer servers to set their preferences and monitor quarantine messages. See Zango, 568 F.3d at 1176 (finding defendant antivirus software provider entitled to CDA immunity because defendant provided anti-malware software and "provided . . . customers with online access to . . . update servers.").

Finally, Microsoft's EHS service "make[s] available to information content providers . . . the technical means to restrict access to" harassing and objectionable material. 47 U.S.C. § 230(c)(2)(B). As this Court held in Smith I, spam email may constitute harassing or objectionable material within the meaning of Section 230. 2010 WL 1799456, at *6. Because Microsoft's EHS service provides internet service providers with the means to restrict access to unwanted spam email, Microsoft's activities fall within the realm of conduct protected by the CDA.

Therefore, because Microsoft is the user and provider of an interactive computer service,

and Microsoft's EHS service provides Comcast with a means to restrict access to harassing spam email, Microsoft is immune to liability under the CDA as a matter of law. Accordingly, Plaintiff's NJCFA, breach of contract, and defamation claims against Cisco are dismissed.[8]

3. Comcast

In Smith I, this Court held that Comcast is not entitled to Good Samaritan immunity under Section 230 because the Complaint alleged sufficient facts to warrant the inference that Comcast acted in bad faith when it blocked Plaintiff's outgoing emails. 2010 WL 1799456, at *7. The Court highlighted the fact that after Plaintiff complained to Comcast, Comcast replied by informing Plaintiff that "[he] would not have to worry about any e-mail blocking if [he] subscribed to a higher level of service." (Compl. ¶ 39). Comcast now argues that it is entitled to an inference of good faith because the Second Amended Complaint fails to allege that Comcast told Plaintiff that he would not have to worry about e-mail blocking if he subscribed to a different level of service, and Comcast's service agreement immunizes it from liability for monitoring Internet service. (Def.'s Mot. Br., at 28).

The Court finds that a reasonable jury could conclude that Comcast acted in bad faith when it failed to respond to Plaintiff's repeated requests for an explanation why it continually blocked Plaintiff's outgoing email. Notwithstanding the fact that Plaintiff no longer alleges that Comcast told him that he would not have to worry about email blockages if he subscribed to a higher level of service, the Court finds no explanation for Comcast's failure to respond after Plaintiff contacted Comcast to ascertain the reason for the second blockage. Put simply, the Court is not convinced that an internet service provider acts in good faith when it simply ignores a subscriber's request for information concerning an allegedly improper email blockage.

[8] The Court notes that Plaintiff's breach of contract claim against Microsoft is dismissed because it relates specifically to Microsoft's EHS. Plaintiff's breach of contract claim is based on the fact that Microsoft refused to provide Plaintiff with the information that it used to determine whether to block Plaintiff's email. (Id. ¶ 2).

Moreover, even if, as Comcast argues, the Subscriber Agreement precludes Comcast from liability for monitoring Plaintiff's emails, there is no reason why Comcast could not articulate its immunity (or provide another rationale for the blockage) when asked to do so by a paying customer. Therefore, because a reasonable jury could conclude that Comcast acted in bad faith when it failed to respond to Plaintiff's requests, Comcast is not entitled to immunity under the CDA.

B. The Wiretap Act

The Wiretap Act provides that "[e]xcept as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; . . . shall be subject to suit as provided in subsection (5)." 18 U.S.C. § 2511(1)(a). The Act further provides for civil liability as follows: "[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2520(a).

However, the Wiretap Act contains an express exemption for interceptions made with the express consent of one party to the communication. Section 2511(1)(a) provides in relevant part:

> It shall not be unlawful under this chapter [] for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(1)(a) (emphasis added). Thus, a non-state actor who intercepts an email communication after receiving consent from one of the parties to the communication is exempt

from liability under the Wiretap Act.

1. Cisco

Plaintiff claims that Cisco violated the Wiretap Act by eavesdropping on his email communications. In particular, Plaintiff claims that Cisco "told Plaintiff [that] they placed network monitoring devices in thousands of networks across the world in order to develop reputation scores for IP addresses." (Second Am. Compl, ¶ 15). Cisco argues that Plaintiff's Wiretap Act claim fails because Plaintiff fails to allege that Cisco intercepted any of his email communications. (Defs.' Br., at 20).

The Court finds that because Plaintiff failed to allege (and there is no evidence in the record) that Cisco intercepted any of his email communications, Plaintiff's Wiretap Act claim fails. As previously mentioned, Cisco's SenderBase service generates reputation scores for individual IP addresses. Based on the reputation score Cisco gave Plaintiff's IP address, Comcast blocked Plaintiff's outgoing email. There is no evidence that Cisco actually intercepted and monitored Plaintiff's email communications in order to generate the reputation score it gave Plaintiff's IP address. Therefore, because Plaintiff fails to put forth evidence that Cisco monitored his outgoing email, Cisco is entitled to summary judgment on Plaintiff's Wiretap Act claim.

2. Microsoft

Plaintiff claims that Microsoft violated the Wiretap Act by eavesdropping on his internet communications. Specifically, Plaintiff claims that Microsoft "collected e-mail messages from Plaintiff and . . . archived the 'To' and 'From' fields," of Plaintiff's emails. (Second Am. Compl. ¶ 15). Microsoft argues that Plaintiff's Wiretap Act claim fails because (1) the Wiretap Act excludes communications made with the consent of one party, and (2) there is no evidence

that Microsoft intercepted his emails for a criminal or tortious purpose. (Defs.' Br., at 21). The Court agrees.

Plaintiff's Wiretap Act claim against Microsoft fails because the Wiretap Act expressly exempts interceptions between two parties where one of the parties to the communication gives prior consent to the consented interception. 18 U.S.C. § 2511(1)(a). Here, the record demonstrates that by subscribing to EHS, each Microsoft customer consents to Microsoft intercepting and filtering all of his email communications. That consent alone defeats Plaintiff's claim that Microsoft unlawfully intercepted his outgoing email transmissions. Moreover, it is clear that Microsoft did not intercept Plaintiff's email for a criminal or tortious purpose. Microsoft intercepted Plaintiff's email to protect its customers from unwanted spam. Indeed, as Plaintiff acknowledges in the Second Amended Complaint, Microsoft notified Plaintiff that it blocked his e-mails to prevent them from reaching its customers' inboxes. (Second Am. Compl. ¶¶ 2, 15).

Therefore, because Microsoft customers consented to filtering Plaintiff's email, and there is no evidence that Microsoft blocked Plaintiff's email for any criminal or tortious purpose, Microsoft is entitled to summary judgment on Plaintiff's Wiretap Act claims.[9]

[9] The New Jersey Wiretapping and Electronic Surveillance Control Act (the "New Jersey Wiretap Act") is modeled after the Federal Wiretap Act. See Pascale v. Carolina Freight Carriers Corp., 898 F. Supp. 276, 281 (D.N.J. 1995) (noting that "the legislative intent [of the New Jersey Wiretap Act] . . . was simply to follow the federal [Wiretap Act]") (quoting State v. Fornino, 539 A.2d 301, 307 (N.J. Super. Ct. App. Div. 1988)); see also PBA Local No. 38 v. Woodbridge Police Dep't, 832 F. Supp. 808, 824 (D.N.J. 1993) ("In determining what construction to give to the New Jersey Wiretap Act, the court must weigh the fact that the Act was closely modeled after and made to substantially parallel the Federal Wiretap Act."). As Defendants correctly note in their brief, in Pascale, the Court relied on cases interpreting the Federal Wiretap Act while construing state law provisions containing "virtually identical" language. 898 F. Supp. at 281.

Here, the applicable language in the Wiretap Act is substantially similar to the language in the relevant sections of the New Jersey Wiretap Act. Compare 18 U.S.C. §§ 2510(4); 2511(1), 2(a)(i), (2)(d) with N.J. Stat. Ann. 2A:156A-2(c); 156A-3; 156A-4(a), (d). Therefore, because the Court granted Microsoft and Cisco summary judgment on Plaintiff's Wiretap Act claims, the Court will grant Microsoft and Cisco summary judgment on Plaintiff's New Jersey Wiretap Act claims.

C. Breach of Contract[10]

To succeed on a breach of contract claim in New Jersey, a party must prove that: (1) the parties entered into an agreement, (2) the promisee satisfied the terms of the agreement, (3) the promissor failed to satisfy at least one term of the agreement, and (4) the breach caused the plaintiff to suffer a loss. Cargill Global Trading v. Applied Dev. Co., 706 F. Supp. 2d 563, 579 (D.N.J. 2010). "The party bringing the action [for breach of contract] has the burden of establishing each element in order to establish breach of contract." Id. (citing Nolan v. Control Data Corp., 579 A.2d 1252, 1262 (N.J. Super. Ct. App. Div. 1990)).

Plaintiff alleges that Comcast breached its privacy statement by refusing to allow Plaintiff to review personally identifiable information collected about him. In addition, Plaintiff alleges that Comcast violated its "network management policy" by blocking Plaintiff's port with "the intent of blocking a specific protocol and caus[ing] monetary loss [to Plaintiff]." (Second Am. Compl. ¶ 20). Comcast argues that Plaintiff's breach-of-contract claim fails because Plaintiff violated the terms of the Subscriber Agreement, which specifically prohibits him from using the Comcast high speed internet (HSI) for a business enterprise. (Def.'s Br. in Supp. of Their Mot. to Dismiss, at 11).

The Court finds that no reasonable jury could find that Comcast violated any contractual agreement with Plaintiff for the following reasons. First, the documents that govern Plaintiff's relationship with Comcast grant Comcast the authorization to monitor Plaintiff's internet activity

[10] In the document filed by Plaintiff entitled "Opposition to Summary Judgment Motion by Defendants Cisco and Microsoft," (Doc. No. 95), Plaintiff argues that that the Court should prohibit Comcast from evading its contractual obligations under the doctrine of promissory estoppel. In order to succeed on a promissory estoppel claim in New Jersey, a plaintiff must demonstrate: "(1) a clear and definite promise by the promisor; (2) the promise is made with the expectation that the promissee will rely thereon; (3) the promissee in fact reasonably rel[ied] on the promise [;] and (4) detriment of a definite and substantial nature [was] incurred in reliance on the promise." Pop's Cones v. Resorts Int'l Hotel, 704 A.2d 1321, 1324 (N.J. Super. Ct. App. Div. 1998). Here, there is no evidence in the record that Plaintiff relied on a promise that Comcast would provide him with all personally identifiable information (PII) when he purchased Comcast service. Therefore, no reasonable jury could conclude that a contract existed between the parties based upon a doctrine of promissory estoppel.

and cancel Plaintiff's service when appropriate. Plaintiff's relationship with Comcast is governed by the Subscriber's Agreement, the Acceptable Use Policy, and the Customer Privacy Policy (the "Privacy Policy"). The Acceptable Use Policy expressly provides that Comcast customers may not: (1) "transmit unsolicited bulk or commercial messages commonly known as spam"; (2) "use or run dedicated, stand-alone equipment or servers from the Premises that provide network content or any other services to anyone outside of your . . . local area network . . . [such as] e-mail Web hosting, file sharing, and proxy services and servers"; or (3) use Comcast's internet service "for any business enterprise or purpose (whether or not for profit) . . . ." (Friedman Ex. B at 3-6). Moreover, the Subscriber Agreement provides:

> Comcast will provide you with dynamic Internet protocol ("IP") address(es) as a component of HSI [high speed internet] and these IP address(es) can and do change over time. You will not alter, modify, or tamper with dynamic IP address(es) assigned to you or any other customer. <u>You agree not to use a dynamic domain name server or DNS to associate a host name with the dynamic IP address(es) for any commercial purpose</u> . . . .

(Friedman Certif. Ex. A, at 9) (emphasis added). The Subscriber Agreement also provides that subscribers are not permitted to "use HSI for operation as a server site . . . for email hosting . . . [or] <u>for any business enterprise</u>." (<u>Id.</u> at 10) (emphasis added).

The Acceptable Use Policy authorizes Comcast to take certain measures when it suspects that a customer is violating any of its policies. For example, the Acceptable Use Policy provides:

> [I]f the Service is used in a way that Comcast or its suppliers, in their sole discretion, believe violates this Policy, Comcast or its suppliers may take any responsive actions they deem appropriate under the circumstances with or without notice. These actions include, but are not limited to, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Service . . . . <u>Neither Comcast nor its affiliates, suppliers, or agents will have any liability for any of these responsive actions</u>. These actions are not Comcast's

> exclusive remedies and Comcast may take any other legal or technical actions it deems appropriate with or without notice.

(Id. at 9) (emphasis added).

Notwithstanding the clear language of the Subscriber's Agreement and the Acceptable Use Policy, the Second Amended Complaint makes clear that Plaintiff operated a commercial enterprise with his Comcast service. Plaintiff alleged that the mail server he uses to transmit emails to recipients outside of the Comcast network bears the name "keywordfactory.com." (Second Am. Compl. ¶ 12). Plaintiff also alleged that the domain name "keywordfactory.com" is registered in his name, and contains his address, phone number, and e-mail address. (Pl.'s Opp'n Br. ¶ 12). Keywordfactory.com "is a web development company located in Ocean City, New Jersey (near Atlantic City)."[11] See www.keywordfactory.com. Therefore, because Plaintiff configures all email messages from his home computer, including all of his business messages, and uses Comcast HSI to operate his out-of-network email server, Comcast had the contractual authority to block his outgoing email or terminate his service.

Second, Plaintiff's breach-of-contract claim fails because Plaintiff failed to put forth evidence that Comcast is contractually obligated to provide him with PII aside from the information contained in his customer invoices, or, that Comcast breached any contractual obligation by refusing to provide him with "maintenance and complaint information" and "additional service information." The Privacy Policy states: "You may examine and correct, if necessary, the personally identifiable information regarding you that is collected and maintained by Comcast in our regular business records." (First Am. Compl. Ex. AA, at 10). The Privacy

[11] Indeed, the First Amended Complaint alleges that "Plaintiff owns and operates a Limited Liability Company, The Keyword Factory, LLC (Keyword Factory) that operates web sites. Plaintiff has 100% ownership in Keyword Factory and no employees."). (First Am. Compl. ¶ 8).

Policy defines PII as "information that identifies a particular person," and cites the following examples of PII:

- [a customer's] name;
- service address;
- billing address;
- email address
- telephone number;
- driver's License number;
- Social Security number;
- bank account number;
- credit card number;
- other similar account information.

(Id. at 1). The Privacy Policy also states the Comcast collects "other" information about each customer's account such as: (1) "maintenance and complaint information" and (2) "additional service information." (Id. at 4). Plaintiff claims that Comcast breached the parties' agreement by refusing to give him access to "maintenance and complaint information" and "additional service information." (Second Am. Compl. ¶ 24). However, neither "maintenance and complaint information" nor "additional service information" is information that personally identifies an individual, and Plaintiff offers no basis for his contention that the Court should classify those items as PII. Thus, the Court is unconvinced that by denying Plaintiff access to "maintenance and complaint information" and "additional service information" Comcast breached any of its contractual obligations. Moreover, Comcast provided Plaintiff with customer invoices that contain ordinary PII – such as the customer's name, account number, address, etc. Thus, there is no factual basis for Plaintiff's assertion that Comcast failed to provide him with PII.

Therefore, because Plaintiff fails to offer evidence that Comcast refused to provide him with PII, or unlawfully monitored and blocked his email transmissions, Comcast is entitled to summary judgment on Plaintiff's breach of contract claim.

D. The New Jersey Consumer Fraud Act

Plaintiff alleges that "[a]ll Defendants have violated the NJCFA by false and misleading advertising involving a consumer transaction." (Second Am. Compl. ¶ 22). With respect to Comcast, the Second Amended Complaint alleges that Comcast falsely advertised its privacy statement and network management policy by denying him access to all of his PII. (Id.). In addition, Plaintiff claims that "Comcast . . . continued to provide Plaintiff with 'defective' IP addresses that have poor reputation scores . . . ." (Id.). Comcast argues that Plaintiff's NJCFA claim fails because (1) Plaintiff failed to allege an unlawful practice as defined by N.J. Stat. 56:8-2, and (2) Plaintiff failed to allege an ascertainable loss resulting from Comcast's allegedly unlawful conduct.

The NJCFA provides protection to consumers from "fraudulent practices in the marketplace." Furst v. Einstein Moomjy, Inc., 860 A.2d 435, 440 (N.J. 2004). In order to further its remedial purpose, the NJCFA is "construe[d] liberally to accomplish its broad purpose of safeguarding the public." Id. at 441. Under the NJCFA, "[a] consumer who proves (1) an unlawful practice, (2) an 'ascertainable loss,' and (3) a causal relationship between the unlawful conduct and the ascertainable loss,' is entitled to legal and/or equitable relief, treble damages, and reasonable attorneys' fees." Lee v. Carter-Reed Co., LLC, 4 A.3d 561, 576 (N.J. 2010). The NJCFA defines an unlawful practice as "any unconscionable commercial practice, deception, fraud, false pretense, false promise, [or] misrepresentation . . . in connection with the sale or advertisement of any merchandise . . . ." N.J. Stat. Ann. 56:8-2.

A plaintiff must plead an NJCFA claim based upon an alleged fraud or misrepresentation with particularity. See Fed. R. Civ. P. 9(b); Maniscalco v. Brother Int'l Corp. (USA), 627 F. Supp. 2d 494, 500 (D.N.J. 2009); Slim CD, Inc. v. Heartland Payment Sys., No. 06-2256, 2007

WL 2459349, at *11 (D.N.J. Aug. 22, 2007) (citing F.D.I.C. v. Bathgate, 27 F.3d 850, 856 (3d Cir. 1994)). In order to satisfy that standard, a plaintiff must "allege the date, time and place of the alleged fraud or otherwise inject precision or some measure of substantiation into a fraud allegation." Maniscalco, 627 F. Supp. 2d at 500.

Plaintiff's NJCFA claim fails because there is no evidence in the record that Comcast denied him any PII, or that Comcast engaged in any fraud, deception, or sharp practice by blocking his email communications based upon the poor reputation score of his IP address. First, Plaintiff's claim that Comcast denied him PII is without merit. As previously mentioned, Comcast provided Plaintiff with all of his invoices. Plaintiff's invoices contain his name, account number, address and other personal information. Plaintiff offers no basis for the assertion that Comcast denied him any personal information; rather Plaintiff proceeds upon the unsupported assertion that Comcast possessed other PII which it refused to provide him upon request. Second, there is no evidence that Comcast singled Plaintiff out from all of its other customers and purposefully provided him with "defective" IP addresses. Plaintiff's claim that Comcast "continued to provide [him] with defective IP addresses that have poor reputation scores" amounts to nothing more than pure speculation and conjecture. (Second Am. Compl. ¶ 22).

Furthermore, even assuming arguendo that there is a material issue of fact concerning whether Comcast engaged in an unlawful practice, Plaintiff's NJCFA claim fails because no reasonable jury could find that Plaintiff suffered "ascertainable loss" as a result of Defendants' allegedly unlawful conduct. An ascertainable loss is a "quantifiable or measurable" loss, not a "hypothetical or illusory" loss. Lee, 4 A.3d at 576; see Thiedmann v. Mercedes-Benz USA, LLC, 872 A.2d 783, 792 (2005). A plaintiff who fails to prove ascertainable loss cannot succeed

on an NJCFA claim. Weinberg v. Sprint Corp., 173 N.J. 233, 249-50 (2002); see Dabush v. Mercedes-Benz USA, LLC, 874 A.2d 1110, 1116 (N.J. Super. Ct. App. Div. 2005) ("a private plaintiff must demonstrate an ascertainable loss of moneys or property, real or personal, as a result of the defendant's unlawful conduct."). "In cases involving breach of contract or misrepresentation, either out-of-pocket loss or a demonstration of loss in value will suffice to meet the ascertainable loss hurdle and will set the stage for establishing the measure of damages." Thiedmann, 872 A.2d at 792. A plaintiff need not calculate the exact measure of damages. Id. However, at minimum, a plaintiff must provide "an estimate of damages, calculated within a reasonable degree of certainty.'" Id. (internal quotations omitted).

The only "loss" Plaintiff alleges is the value of his personal time. The Second Amended Complaint alleges that Plaintiff suffered monetary loss from "conduct[ing] extensive troubleshooting to try to solve the problem and avoid future incidents." (Second Am. Compl. ¶ 9). The Second Amended Complaint also alleges that Plaintiff devoted time to "identify[ing] and correct[ing] the problem" with his email by "scanning [his] home computer for malicious software, checking log files, checking configurations, and conducting Internet searched [sic] to try to determine the cause of the problem." (Id. ¶ 9 n.6). However, aside from the mere inconvenience of troubleshooting an email glitch, Plaintiff fails to offer evidence of an ascertainable loss resulting from his efforts to remedy the blockage of his email communications. There is no evidence that Plaintiff suffered any out-of-pocket loss or loss in value. Put simply, the only time Plaintiff lost was the time that he would have spent conducting his internet business but for the email blockage. That inconvenience is insufficient to satisfy the NJCFA's ascertainable loss requirement. Accordingly, Comcast is entitled to summary judgment on Plaintiff's NJCFA claim.

E. Cable Communications Policy Act

Comcast moves to dismiss Plaintiff's claim based on the Cable Act. Comcast argues that Plaintiff fails to allege any basis for the conclusion that he was denied access to any PII because Comcast offered him access to his customer invoices. The Court agrees.

Under the Cable Act, a cable operator has a host of responsibilities, the violation of which are actionable in a civil suit. 47 U.S.C. § 551. Among those responsibilities is a duty to provide cable subscribers with access to all PII about the subscriber that the cable operates, collects, and maintains. 47 U.S.C. § 551(d). The Cable Act does not define what such information is, but does state what it is not: "the term 'personally identifiable information' does not include any record of aggregate data which does not identify particular persons." § 551(a)(2)(A). One court has noted that the legislative history to the Cable Act states that personally identifiable information "include[s] specific information about the subscriber, or a list of names and addresses on which the subscriber is included . . . ." Scofield v. Telecable of Overland Park, Inc., 973 F.2d 874, 876 n. 2 (10th Cir. 1992) (internal quotations omitted). Another court has held that a person's name, address, and telephone are quintessential PII. Warner v. Am. Cablevision of Kansas City, Inc., 699 F.Supp. 851, 855 (D.Kan.1988); see also Pruitt v. Comcast Cable Holdings, LLC, 100 Fed. App'x. 713, 716 (10th Cir.2004) (finding cable box did not contain personally identifiable information where, inter alia, it did not contain the name, address, or "any other information regarding the customer").

The Court that finds because Comcast gave Plaintiff access to his invoices, no reasonable jury could find that Comcast denied him access to any PII. The Second Amended Complaint alleges that after Plaintiff contacted Comcast to determine why Comcast blocked his emails, Comcast refused to give him access to any of his account information; and instead gave him

access to his customer invoices. Furthermore, Plaintiff argues in the Opposition Brief that Comcast collected "maintenance and complaint information" and "additional service information". (Second Am. Compl. ¶ 24). However, neither "maintenance and complaint information" nor "additional service information" is information that personally identifies Plaintiff. By contrast, it is readily apparent that the information available on a standard invoice such as Plaintiff's name, account number, address, etc. – information Comcast readily provided to Plaintiff – constitutes PII. Therefore, because Plaintiff failed to offer evidence that the information Comcast withheld from him was PII, Comcast is entitled to summary judgment on Plaintiff's Cable Act claim.

F. Ocean City Franchise Ordinance #07-33

Comcast moves to dismiss Plaintiff's Ocean City Franchise Ordinance #07-33 ("Ordinance #07-33") claim. Comcast argues that because no private remedy exists under Ordinance #07-33, Plaintiff's claim fails as a matter of law. The Court agrees.

Ordinance #07-33, grants Comcast the right to provide internet services to customers in Ocean City, New Jersey. Section 9 of the Ordinance states that "[i]n providing services to its customers, [Comcast] shall comply with . . . all applicable state and federal statutes and regulations." Ordinance #07-33 § 9. However, Ordinance #07-33 provides no private right of action for Comcast subscribers. Specifically, Ordinance #07-33 states that:

> In the event that the Municipality shall find that [Comcast] has not substantially complied with the material terms and conditions of this Ordinance, the Municipality shall have the right to petition the OCTV [Office of Cable Television], pursuant to N.J.S.A. 48:5A-47, for appropriate action, including modification and/or termination of the Certificate of Approval; provided however, that the Municipality shall first have given the Company written notice of all alleged instances of non-compliance and an opportunity to cure same within ninety (90) days of that notification.

Thus, under the express terms of Ordinance #07-33, the only remedy available for an alleged violation is for the Municipality to petition the Office of Cable Television of the New Jersey Board of Public Utilities. Because the Ordinance does not create a separate cause of action for individual subscribers of Comcast service, the Court will grant Comcast summary judgment on Plaintiff's Ordinance #07-33 claim.

III. CONCLUSION

For the reasons discussed above, summary judgment is granted in favor of Defendants Cisco, Microsoft, and Comcast on all claims against them. An appropriate order shall issue today.

Date: 3/15/2011

/s/ Robert B. Kugler
ROBERT B. KUGLER
United States District Judge